A hybrid framework for detecting and eliminating cyber-attacks in power grids

Arshia Aflaki, Mohsen Gitizadeh, Roozbeh Razavi-Far, Vasile Palade, and Ali Akbar Ghasemi

Original citation & hyperlink:
Aflaki, A., Gitizadeh, M., Razavi-Far, R., Palade, V. and Ghasemi, A.A., 2021. A Hybrid Framework for Detecting and Eliminating Cyber-Attacks in Power Grids. *Energies*, *14*(18), 5823.
https://doi.org/10.3390/en14185823

DOI **10.3390/en14185823**
ISSN 1996-1073

Publisher: MDPI

energies

MDPI

Article

A Hybrid Framework for Detecting and Eliminating Cyber-Attacks in Power Grids

Arshia Aflaki [1], Mohsen Gitizadeh [1,*], Roozbeh Razavi-Far [2], Vasile Palade [3] and Ali Akbar Ghasemi [1]

[1] Department of Electronics and Electrical Engineering, Shiraz University of Technology, Shiraz 71555-313, Iran; arshiaaflaki@gmail.com (A.A.); aa.ghasemi@sutech.ac.ir (A.A.G.)
[2] Department of Electrical and Computer Engineering, University of Windsor, Windsor, ON N9B 3P4, Canada; roozbeh@uwindsor.ca
[3] Center for Data Science, Coventry University, Coventry CV1 5FB, UK; vasile.palade@coventry.ac.uk
* Correspondence: gitizadeh@sutech.ac.ir

Abstract: The work described in this paper aims to detect and eliminate cyber-attacks in smart grids that disrupt the process of dynamic state estimation. This work makes use of an unsupervised learning method, called hierarchical clustering, in an attempt to create an artificial sensor to detect two different cyber-sabotage cases, known as false data injection and denial-of-service, during the dynamic behavior of the power system. The detection process is conducted by using an unsupervised learning-enhanced approach, and a decision tree regressor is then employed for removing the threat. The dynamic state estimation of the power system is done by Kalman filters, which provide benefits in terms of the speed and accuracy of the process. Measurement devices in utilities and buses are vulnerable to communication interruptions between phasor measurement units and operators, who can be easily manipulated by false data. While Kalman filters are incapable of detecting the majority of such cyber-attacks, this article proves that the proposed unsupervised machine learning method is able to detect more than 90 percent of the mentioned attacks. The simulation results on the IEEE 9-bus with 3-machines and IEEE 14-bus with 5-machines systems verify the efficiency of the proposed approach.

Keywords: cyber-attacks; dynamic state estimation; hierarchical clustering; Kalman filter; unsupervised learning

Citation: Aflaki, A.; Gitizadeh, M.; Razavi-Far, R.; Palade, V.; Ghasemi, A.A. A Hybrid Framework for Detecting and Eliminating Cyber-Attacks in Power Grids. *Energies* **2021**, *14*, 5823. https://doi.org/10.3390/en14185823

Academic Editor: Mohamed Benbouzid

Received: 30 July 2021
Accepted: 10 September 2021
Published: 15 September 2021

1. Introduction

Many industries are becoming more modernized as technology advances, including the power systems [1]. High-speed internet is being used as the primary mean of communication between various sectors of the power grid. Cyber-attacks pose a significant threat to various industries, as technologies increasingly rely on wireless communications, and most of the power system operations, such as energy management programs, state estimation, optimal power flow, etc., depend on safe and reliable communications [2,3]. DSE is an important tool for monitoring and controlling the power network, especially when the system is performing in the transient mode [4]. DSE is an effective method to track the behavior of the power system in the transient mode, and it usually employs Kalman filters to perform the state estimation process. Modernized power systems, known as smart grids, rely heavily on wireless communication, making them vulnerable to cybercriminals who can tamper with data derived from PMUs [5]. DSE usually uses PMU data as inputs for estimation of the dynamic behavior of the power system, and thus the communication between PMUs and central control is of paramount importance due to vulnerability to cyber-attacks.

Because traditional methods based on various types of Kalman filters are only effective against certain types of cyber-sabotages [5], a machine learning-enhanced method is needed for optimizing the detection process of these attacks. In this article, clustering and

regression techniques are used to tackle these threats, and the results are compared to the previous methods of system defense against the mentioned attacks. While the traditional power system is transitioning to a new and more intelligent system known as the smart grids, the threat posed by cybercriminals is unavoidable, and by injecting more sophisticated attacks, linear and non-linear traditional detection techniques, such as Kalman filters, appear to be rendered ineffective.

Kalman filters were first used in the 1970s, when the term "Dynamic State Estimation" was introduced [6]. With the development of related techniques, more advanced filters were used for the accurate and robust estimation of dynamic states. In recent years, some studies emphasized that DSE fulfills an essential function in dealing with electromechanical transient models and unknown inputs collected from PMUs [7,8]. Numerous methods for detecting and eliminating cyber-sabotages were implemented, ranging from linear techniques to AI-based methods [9–11]. Applying different types of Kalman filters, such as UKF and EKF, to eliminate the malfunctions and unknown data injections was proposed in recent years, and these filters were examined in various scenarios of cyber-attacks [11,12]. While cyber threats are increasing these days, a power system needs better preparation for such attacks. FDI and DoS are two typical kinds of attacks, and while both FDI and DoS consider the measurement equipment as the main target of data injection, the former usually changes the mean value of the measured object, while the latter denies the transmission of data. FDI poses a considerable threat to network security, and by changing the value of the measured data, it misleads the operators via the fundamental change in the monitored states of the system. The situation worsens when it comes to transient electromechanical states. DoS attacks manipulate the power system observers during the transient period of the system and may lead to huge power outages by the incorrect decisions made by operators due to the false data injected by intruders. In 2019, a confirmed case of cyber-attack happened in the US power grid, in which the intruders tried to manipulate the operators by aiming some sensitive PMUs in the power network [13]. Clustering and classification techniques, on the other hand, can be used to provide a more optimized mean of facing these cyber-attacks [2,3]. These days, numerous AI-enhanced techniques are utilized to separate standard data from anomalous ones, which is called anomaly detection. HC is a well-known clustering method used on continuous data and time series [14]. Many classification techniques were proposed in the field of machine learning. Many of them, however, are not suitable for processing challenging time series data. DTR and neighboring techniques seem to be more useful in the case of continuous data generated in power networks.

It is known that the Kalman filter performs well under specific conditions, such as Gaussian-based noise [15]. However, in more complex situations, Kalman filters are struggling to detect the outliers, especially when the measurement noise does not obey the Gaussian assumption [16]. In [17], robust filters were implemented to tackle this problem by using the RCKF and CKF during electromechanical transients in the power transmission network. A non-linear control loop-based method was proposed in [18] as a technique to detect and eliminate cyber-attacks along with risk mitigation.

Wang et al. [19] mention a Luenberger method for both cyber-attack detection and power system isolation. In recent years, the use of AI techniques has boosted power engineering, as demonstrated in [20] by the use of sequential hypothesis testing based on machine learning methods. In [21], the authors propose a machine learning-aided dynamic state estimation method, and in [22], the authors employ a variety of deep learning-based methods to detect false data injection. Ref. [23] reviews how to control the power system under cascading failures. In [24], a new Markov-based approach is proposed to detect DoS attacks, while in [25], applications of extended Kalman filter is illustrated. An online DSE method is proposed in [26]. Ref. [27] uses novel Kalman filters to perform DSE. Reference [28] introduces hierarchical clustering applications for anomaly detection. Basics of random tree for classification and regression was first introduced in [29], and in [30], the authors used the random tree method to recovering clusters under random noise.

In Towards Data Science, Lorraine Li used decision tree for regression and classification problems [31], and in [32], the authors propose a power system toolbox for MATLAB. An EKF/UKF toolbox is proposed in [33]. In [34], a toolbox named PSAT is proposed for dynamic analysis of the power system. It is worth noting that all of the mentioned toolboxes are employed for simulating our results in this paper.

Reference [35] proposes a machine learning-based approach to detect FDI attacks in the power system. In [36], the authors propose a linear approach to detect cyber-attacks and outliers in PMU-based power system state estimation, and in [37], a supervised learning-based approach is proposed to detect DoS attacks in smart grids. Table 1 shows a comparison of the methods studied in this article and others in the same field. As illustrated in Table 1, this article contributes to the field in at least two ways. Firstly, it employs two machine learning-based methods to detect and eliminate the cyber-threats. Secondly, it draws a comparison between Kalman filters and a proposed hybrid machine learning method for the same purpose.

Table 1. Comparison between related studies.

Features	[12]	[15]	[17]	[18]	[36]	[37]	This Article
Supervised learning method	×	×	×	×	×	√	√
FDI attack	√	√	√	√	√	×	√
DoS attack	√	√	√	√	×	√	√
Unsupervised learning method	×	×	×	×	×	×	√
Cyber-attack detection	√	√	√	√	√	√	√
Cyber-attack elimination	√	√	√	√	√	×	√

The rest of this paper is organized as follows. Section 2 formulates models for DSE, fourth-order generator, cyber-attacks and the two Kalman filters utilized for simulation. Machine learning methods are described in Section 3. In Section 4, the proposed approach is detailed, and in Section 5 the proposed method is examined by different case studies, with the results of the simulations being illustrated as well. The paper is concluded in Section 6.

2. Methods

This section firstly presents the generator model of the power system and then describes attack models.

2.1. DSE and the Generator Model

The procedure for estimating the dynamic state of a power system is relatively well known and can be found in many related articles [12,18,23–26]. The relationship between the system's dynamic states and the measurements is formulated as follows:

$$\begin{cases} x_{k+1} = f(x_k,\ u_k,\ v_k) \\ y_{k+1} = h(x_{k+1},\ u_{k+1},\ w_k) \end{cases} \tag{1}$$

where x is the vector containing the states of the system, y is the measurements vector, u refers to the control vector, v is the process noise, w represents the measurement noise, and k is the number of iterations. Both h and f are non-linear state and measurement functions, illustrated in (3) and (4). It is worth noting that in this article, we assume that x, y, and u are shaped as follows.

$$\begin{cases} x = \{\delta,\ \omega\} \\ y = \{P_e,\ P_m,\ \omega^y,\ U,\ \varphi\ \} \\ u = \left\{E_f,\ T_m\right\} \end{cases} \tag{2}$$

where δ, ω are the rotor angle and rotor speed, respectively. ω^y is the measurement of the rotor speed, P_e is the electrical power of the generator, and P_m is the mechanical input power of a generator. U and φ represent the voltage magnitude and phase angle

of the respective bus, E_f is the field voltage of the synchronous generator, and T_m is the mechanical torque derived from the governor.

The fourth-order transient swing equations are formulated below [12,18,23–26].

$$\begin{cases} \dot{\delta} = \omega - 1 \\ \dot{\omega} = \frac{1}{T_J}[T_m - T_e - D(\omega - 1)] \\ \dot{E'}_d = \frac{1}{T'_{d0}}\left[E_f - E'_q - (X_d - X'_d)i_d\right] \\ \dot{E'}_q = \frac{1}{T\prime_{q0}}\left[-E'_d + (X_q - X'_q)i_q\right] \end{cases} \tag{3}$$

T_J represents the inertia time constant, while T_e is the electromagnetic torque, and D is the damping coefficient. X_d and X_q are d-axis and q-axis reactances, respectively, while X'_d and X'_q are d-axis and q-axis transient reactances. T'_{d0} and T'_{q0} are d-axis and q-axis transient time constants. i_d, i_q are d-axis and q-axis output currents and E'_d, E'_q are d-axis and q-axis voltages of a generator.

The measurement vector, which includes δ, ω, and P_e, is listed below [12,18,23–26].

$$\begin{cases} \delta^y = \delta \\ \omega^y = \omega \\ P_e^y = \frac{U^2}{2}\sin(2\delta - 2\varphi)\left(\frac{1}{X'_q} - \frac{1}{X'_d}\right) + \frac{U\sin(\delta - \varphi)E'_q}{X'_d} + \frac{U\sin(\delta - \varphi)E'_d}{X'_q} \end{cases} \tag{4}$$

where δ^y is the measurement of the rotor angle, and P_e^y is the measurement of the electrical power.

Both E_f and T_m are control features that can be obtained from governor and exciter models depending on the power utility, and in both IEEE 9-bus and IEEE 14-bus systems, the power utilities are assumed to be steam power plants. For the random noises, v along with w were calculated by random value generation ranging from "Gaussian" to "Central Limit".

In this article, two different Kalman filters for the forecasting and filtering stages are proposed to improve the speed and accuracy of the DSE. Kalman filtering is an algorithm that estimates some unknown variables taking into account the observed measurements over time. Kalman filters have proven themselves in a wide variety of applications, are relatively simple and easy to use, and require little computing power. The primary aim of employing Kalman filters in our study is to make use of the minimization ability of both EKF and UKF in a non-linear space to reduce the covariance of the squared error between estimated and real states. Both of the aforementioned filters take different approaches to accomplishing this task. Both EKF and UKF formulations can be found in [27], and the two final stages of DSE in this paper, i.e., forecasting and filtering, are based on these. Figure 1 depicts the DSE procedure with the addition of EKF and UKF.

2.2. Attack Models

Cyber-criminals can easily manipulate the DSE process by changing the measurement data-driven by PMUs. Numerous attacking scenarios can be obtained in cyber-enhanced sabotage, particularly in dynamic situations ranging from FDI and DoS to spoofing attacks. Malfunctions and bad data frequently cause disasters and significantly impact the power network's monitoring system, which should be held accountable for the grid's smooth operation. This section goes over two different attack scenarios. Figure 2 depicts a brief summary of how cyber-attacks are carried out on power grids.

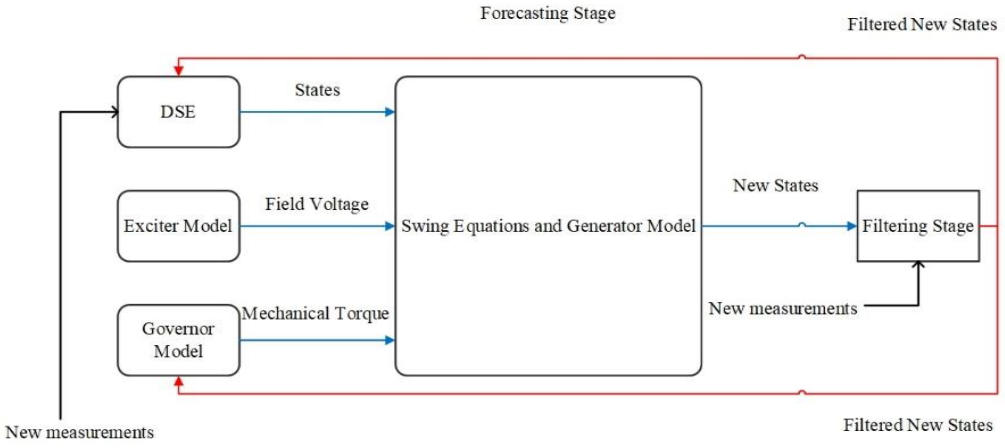


Figure 1. DSE aided by UKF and EKF, in which $x_{t+1 \mid f}$ is the filtered state vector.

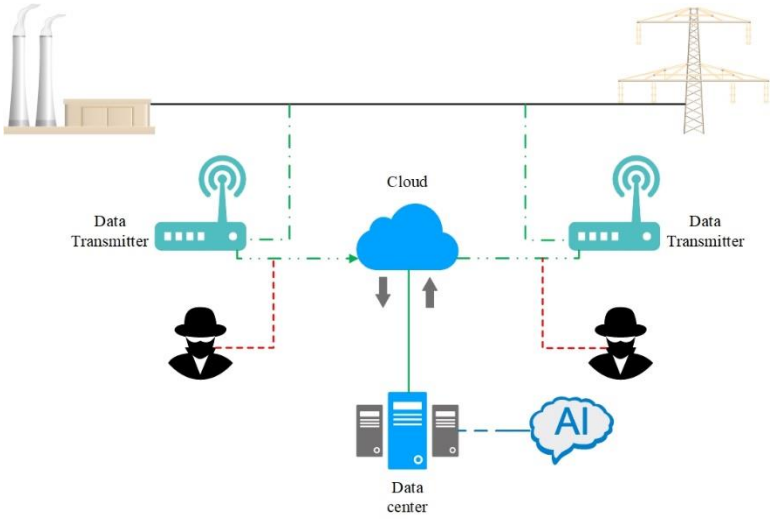


Figure 2. How cyber-attacks can be performed in a smart grid.

2.2.1. FDI Attack

Assume the state vector derived from Kalman filters as $x = [x_1, x_2, x_3, \ldots, x_n]^T$, in which n is the number of states and the measurement vector as $y = [y_1, y_2, y_3, \ldots, y_m]^T$, where m is the number of measurements. The invader targets measurements for the FDI attack because the DSE is highly vulnerable to PMUs records and can be easily manipulated by incorrect data. As shown in (1), measurements are dependent on states and the control vector, so the residual definition can be written as follows:

$$\varepsilon = y - h(x_{k+1}, u_{k+1}, w_k) \tag{5}$$

in which ε is the residual representing the difference between the measured value and the calculated value. It is worth noting that in the optimum situation, the residual is a definite zero. Assume the attack vector as $A = [A_1, A_2, A_3, \ldots, A_m]^T$. The residual under the FDI attack can be calculated as follows:

$$\varepsilon = y + A - h(x_{k+1}, u_{k+1}, w_k) \tag{6}$$

The outcome of the process is an incorrect x which will significantly impact operators for making decisive decisions and may also lead to power outages. In conclusion, while it has the shape of A, the attack has succeeded, and the system states are going to be inaccurate, as illustrated in Figure 3. The subplot in Figure 3 shows how the true measurements are

changing under the FDI attack. As it is illustrated in the mentioned figure, some of the measurements randomly increase or decrease.

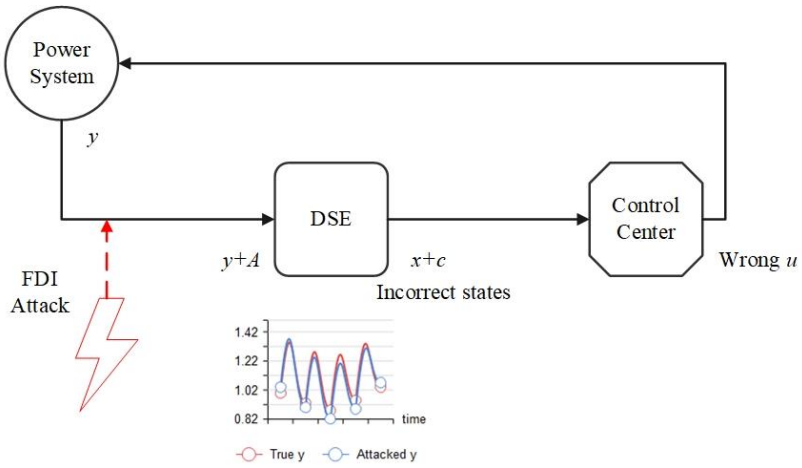


Figure 3. Data under the FDI attack, in which c is the state attack vector.

2.2.2. DoS Attack

This attack is based on data loss, and it can mislead operators by disrupting communication between PMUs and data centers, resulting in power system failures, such as blackouts. A DoS attack can be simulated in a variety of ways, and the Bernoulli distribution [24] method is considered in this article. DoS attacks can be carried out at various intervals or concurrently during the grid's transient time. Assume that $y = [y_1, y_2, y_3, \ldots, y_m]^T$ is the measurement vector in which m is the number of measurements. The interval of DoS attack is assumed to be a vector named t_D, and the attack lasts until t_{Dk}, so the time vector is $t_D = [t_{D0}, t_{D1}, t_{D2}, \ldots, t_{Dk}]$. By employing a Bernoulli distribution, the attack vector of A is described as below.

$$A(i) = \begin{cases} 1 \\ 0 \end{cases} \tag{7}$$

and $i \in [t_{D0}, t_{Dk}]$ while the $var(A(i)) = 1$.

The DoS attack will result in a new measurement vector named y_A. The attacked measurement vector is formulated as follows:

$$y_A = A \times y \tag{8}$$

As in (6), the ε after the DoS attack is going to be calculated as:

$$\varepsilon = y_A - h(x_{k+1}, u_{k+1}, w_k) \tag{9}$$

or

$$\varepsilon = A \times y - h(x_{k+1}, u_{k+1}, w_k) \tag{10}$$

Therefore, by twisting the measured data, DSE will fail to estimate the true states, and operators will be manipulated by the wrong information delivered by DSE at several different times (within t_D). In Figure 4, the mechanism of the DoS attack is illustrated. The subplot in Figure 4 shows how the true measurements change under the FDI attack. As it is illustrated in the mentioned figure, some of the measurements, depending on Bernoulli's probability, become zeros.

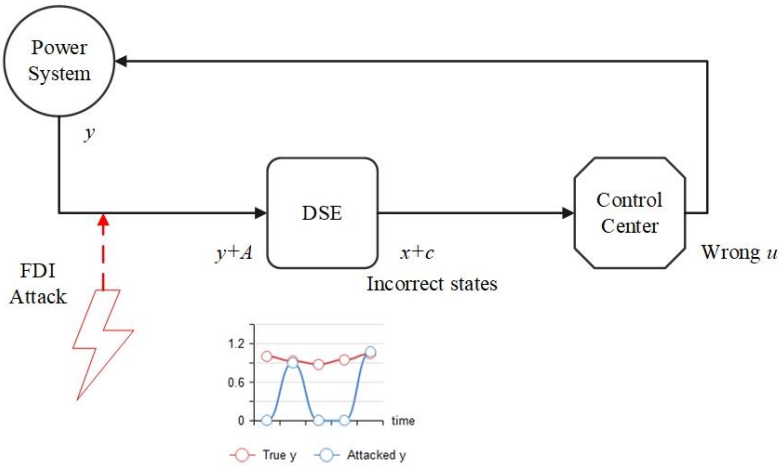


Figure 4. Data under the DoS attack, in which c is the state attack vector.

3. AI-Based Methods

In this article, an unsupervised learning method, HC, and a supervised method, DTR, are employed to facilitate the detecting and eliminating process.

3.1. Hierarchical Clustering

HC is a broad category of clustering algorithms that construct nested clusters by successively merging or splitting them. This cluster hierarchy is portrayed as a tree (or dendrogram). The tree's root is a single cluster that collects all of the samples, while the leaves are clusters with just one sample [28], making the HC a suitable method for detecting the cyber-attack performed in a power system with various sample data derived from PMUs. In this article, the agglomerative type of HC is employed, which is a bottom-up approach. Each discovery begins in its cluster, and when one progresses up the hierarchy, pairs of clusters are combined. Figure 5 represents the dendrogram of agglomerative HC.

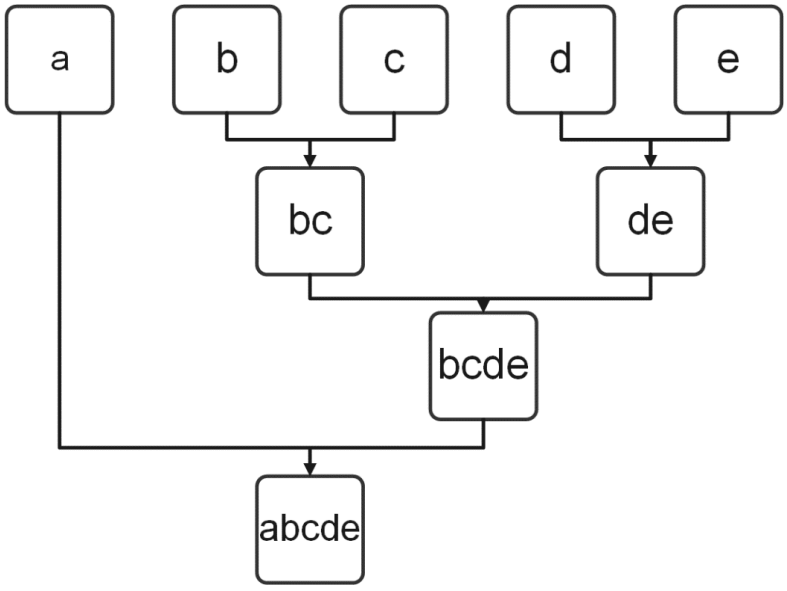


Figure 5. Agglomerative clustering dendrogram, in which squares represent clusters and letters represent data.

The distance metrics for HC range from the Euclidean distance to the Mahalanobis distance. The most common distance metric for agglomerative clustering is the Euclidean

distance. Assume that a and b are two different data vectors. The Euclidean distance is formulated as below.

$$\|a - b\|_2 = \sqrt{\sum_i (a_i - b_i)^2} \tag{11}$$

The linkage criterion determines the distance between sets of observations that includes pairwise distances between observations. Commonly used linkages criteria are complete-linkage clustering and single-linkage clustering. Assume that A and B are two sets of observations. The single-linkage clustering is formulated as below.

$$\text{Linkage} = min\{d(a, b) \ : a \in A, \ b \in B\} \tag{12}$$

where d is the distance metric.

3.2. Decision Tree

Decision trees are a non-parametric supervised learning method for classification and regression tasks [29]. The goal is to learn basic decision rules from data features to construct a model for prediction. Used at the elimination stage, DTR is employed as a prediction method to prevent the manipulation of the operators and the upcoming disasters. A supervised learning technique requires labeled data to train the model with, and, for that purpose, we simulated numerous dynamic events and trained the tree regressor with different non-attacked data. DTR can work with time series and continuous values such as those we are facing in the power networks, making this method well suited for this purpose [30]. DTR does not necessarily require pre-scaling or pre-processing of data, which is useful in the case of generators' angles as the angle is forecasted in degree. Missing values in the power system data also do not affect the process of building a decision tree to any considerable extent. Last but not least, DTR prevents overfitting and boosts the speed of the learning process compared to other methods. Assume a training data set $X = x_1, \ x_2, \ \ldots, \ x_n$ with the responses $Y = y_1, \ y_2, \ \ldots, \ y_n$ in which n is the number of samples. Bagging will create a random sample with replacement to boost the accuracy in B repeats. Therefore, a sample of training data $X_b, \ Y_b, b = 1, 2, \ldots, B$, is created, and the DTR can be fitted with them, and after that, other non-tested samples x' will be predicted. A considerable advantage of DTR is that with respect to the whole forest trained on the bagged datasets, the variance will be decreased without increasing the bias, meaning that the model is not sensitive to noise. The predicted value for test data x' is calculated as follows by assuming f as tree regressor.

$$f = \frac{1}{B} \sum_{b=1}^{B} f_b(x') \tag{13}$$

and the standard deviation can be formulated as below:

$$\sigma = \sqrt{\frac{\sum_{b=1}^{B} (f_b(x') - \ f)^2}{B - 1}} \tag{14}$$

4. Problem Formulation

Both machine learning methods mentioned in the last section are employed to spot and eliminate cyber-attacks. For tackling the cyber-sabotage problem in the power system, a modified version of HC is employed. The main idea behind this approach is to identify the anomalous data and eliminate them and reduce the features used as input to the DTR so that the algorithm predicts the correct states of the system. The challenge of the proposed method is to maintain the high accuracy of its predicted states (rotor angle and rotor mechanical speed), and reducing the dimension of the main features exerts a pervasive influence on the accuracy of this method. The main features chosen in this work are as follows.

$$fea = [P_m, \ U, \ \varphi, \ \omega^z] \tag{15}$$

In which fea is the vector of features, and the clustering distortion is formulated as below [28].

$$J(c,\mu) = \sum_{i=1}^{m} \|s^i - \mu_c(i)\| \tag{16}$$

While s^i is the ith sample, the cluster centroids are μ_c, m is the number of clusters, and $c = [1, 2, 3, \ldots, k]$.

HC is a vital tool for detecting anomalies, and when data is far from other tree roots or leaves, it is usually clustered as an outlier with respect to the threshold set for the method. Therefore, for each measurement type, voltage, speed, etc., an HC algorithm will be utilized to detect the attacked data. As the data derived from PMUs are flowing, the HC accepts the new data and starts clustering. If the data is clustered as an outlier, the algorithm will send it to the DTR, and the regression method replaces the data by using other features and predicts the real value of the attacked data, and then the predicted value will be sent to the DSE, while HC will delete the attacked data from its database. If not an outlier, the data will be sent directly to the DSE for state estimating purposes. We need an impurity metric appropriate for continuous variables to use a decision tree for regression, so we define the impurity measure using the children's leaves' weighted mean squared error (MSE) [31].

$$\text{MSE} = {}^{1}/_{N_t} \sum_{i \in D_t} \left(a^{(i)} - \hat{a}_t\right)^2 \tag{17}$$

$$\hat{a}_t = {}^{1}/_{N_t} \sum_{i \in D_t} a^{(i)} \tag{18}$$

where N_t is the number of samples at the leave t, while D_t is the training subset, $a^{(i)}$ is the true target value and $\hat{a}_t$ is the estimated target value. It is worth noting that the mentioned equations are used for the training process of the DTR. Figure 6 illustrates the flowchart of the proposed method.

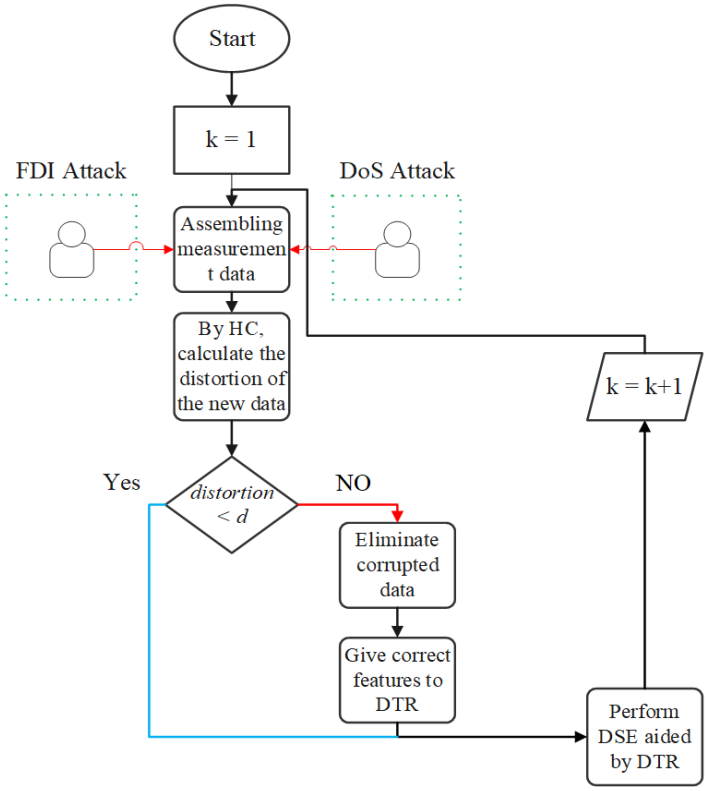


Figure 6. Our proposed method for state estimation, which results in more accurate estimations under cyber-attacks.

For comparing different methods, some indices are defined and used as follows [12,36,37].

$$\tau_1 = \sqrt{\frac{\sum_{i=1}^{N}(\hat{x}_i - x_{itrue})^2}{N}} \tag{19}$$

$$\tau_2 = \frac{S_{ad}}{S_a} \tag{20}$$

$$\tau_3 = \frac{1}{M_c(T - t_0 + 1)} \sqrt{\sum_{i=0}^{t}(\hat{x}_i - x_{itrue})^2} \tag{21}$$

where N is the number of samples while $\hat{x}_i$ and x_{itrue} are estimated and true states, respectively. S_a and S_{ad} are the number of the attacked data and detected attacked data, respectively. M_c is the number of Monte-Carlo replications, which in this article is set to be 100. T and t_0 are the end and the starting time of the period in which the cyber-attack was launched, respectively. It is clear that the first index is able to evaluate the estimation results, while the second one is the attack classification ratio. The last index represents the least squared error measure.

5. Simulation and Results

Here, the proposed method was tested on the IEEE 3-machine 9-bus system and the IEEE 5-machine 14-bus system, while the data of these test systems are derived by using the MATLAB power system toolbox [32] and the EKF and UKF methods are from the EKF/UKF toolbox [33]. All tests are conducted with MATLAB 2020a and Python 3.8. A sudden load fluctuation happened in 0.1 and lasted for 1 s in both test systems. The PMU sample rate is 120 samples per second, and a PMU is utilized at each generator bus.

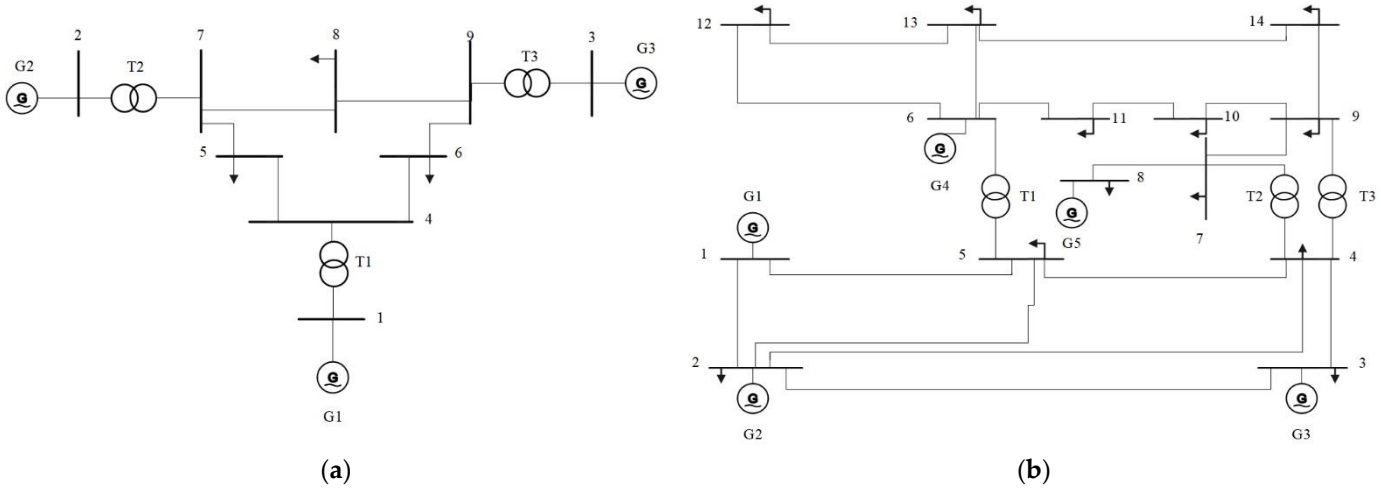
Two case studies are represented in this article, and various cyber-attacks are employed for the simulation process. Both FDI and DoS attacks are simulated with different attack vectors and probabilities as illustrated in Table 2. It is worth noting that the base rotor speed is 376.8 rad/sec for both case studies, and the base generator angle is 1 degree. The cyber-attacks were launched over t = 4.2 s and exerted a significant influence on the DSE. The HC has clustered all the features simultaneously by taking the distortion level of features into account, and the DTR was held responsible for clearing the attack and correcting the states. It is worth noting that the DTR was trained by numerous data from different contingencies ranging from three-phase fault to lightning stroke, all of which are available on a MATLAB power system's toolbox named PSAT [34].

Table 2. Illustrates seven different attack scenarios.

Attack Scenarios	State Attack Vectors Standard Deviation	Packet Loss Rate
FDI–first scenario	$N(0, \sigma)$, $\sigma = 0.0001$	×
FDI–second scenario	$N(0, \sigma)$, $\sigma = 0.001$	×
FDI–third scenario	$N(0, \sigma)$, $\sigma = 0.01$	×
DoS–first scenario	×	1
DoS–second scenario	×	0.95
DoS–third scenario	×	0.85
DoS–fourth scenario	×	0.75

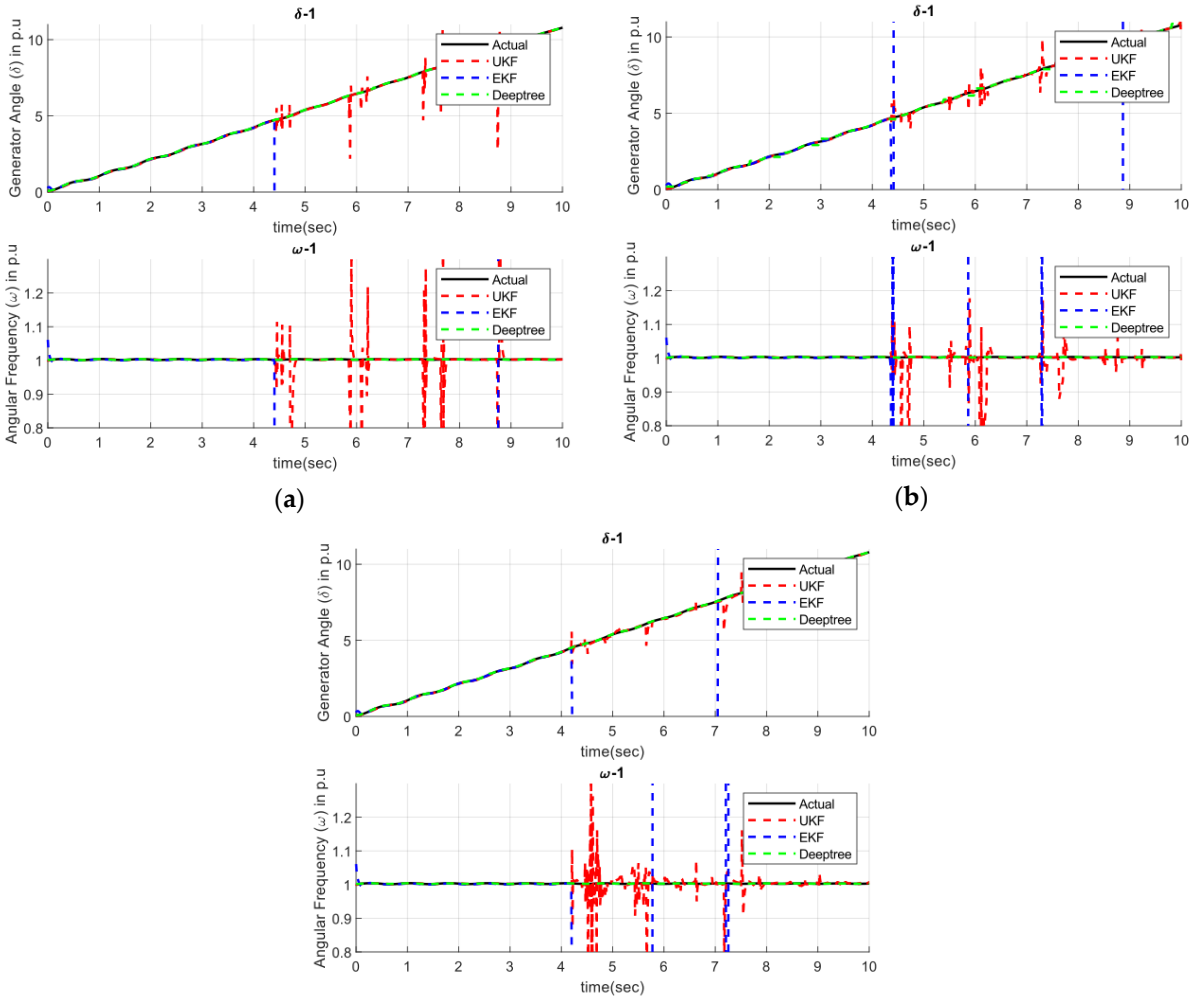
In the three scenarios of FDI cyber-attack, the "Normal Distribution" is employed with different standard deviations for simulating the attacks [35]. In DoS cases, a "Packet Loss Ratio" is utilized for simulating the DoS attack process with four different intensities. Figure 7 shows the schematic of the IEEE 3-machine 9-bus and IEEE 5-machine 14-bus systems. The whole simulation time is about 10 s, while the distortion constant is set to 10 for the IEEE 9-bus and 30 for the IEEE 14-bus. Figure 8 illustrates the first generator's states derived from the DSE, aided by EKF, UKF, and the proposed method under the three FDI cyber-attack scenarios. Figure 9 shows the dynamic states of the mentioned

generator calculated by DSE under DoS cyber-sabotages for the IEEE 3-machine 9-bus test system.



(**a**) (**b**)

Figure 7. (**a**) IEEE 3-machine 9-bus schematic; (**b**) IEEE 5-machine 14-bus schematic.



(**a**) (**b**)

(**c**)

Figure 8. (**a**) Rotor angle and angular frequency of the first generator in IEEE 9-bus system under the FDI attack scenario 1; (**b**) rotor angle and angular frequency of the first generator in IEEE 9-bus system under the FDI attack scenario 2; (**c**) rotor angle and angular frequency of the first generator in IEEE 9-bus system under the FDI attack scenario 3.

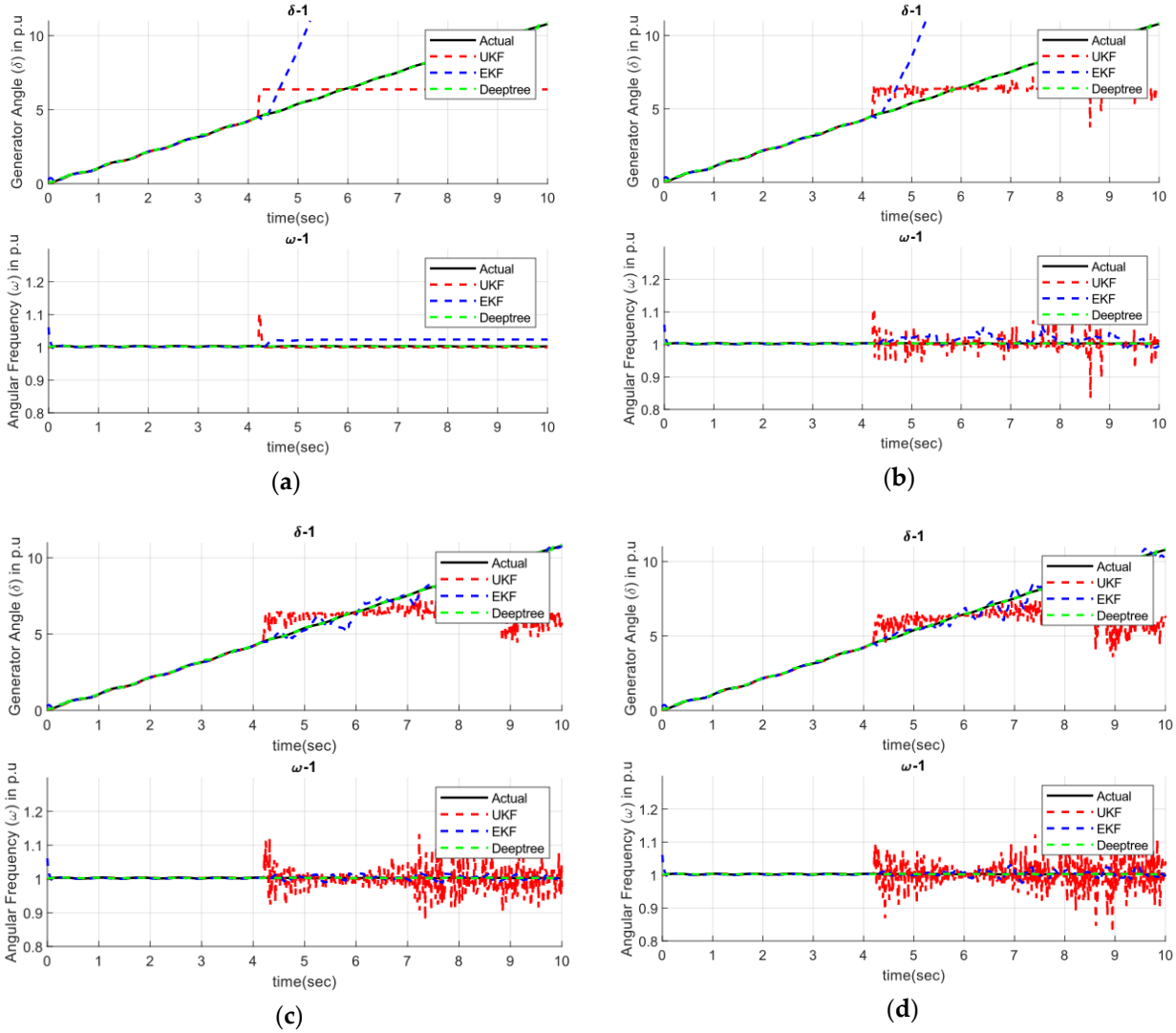
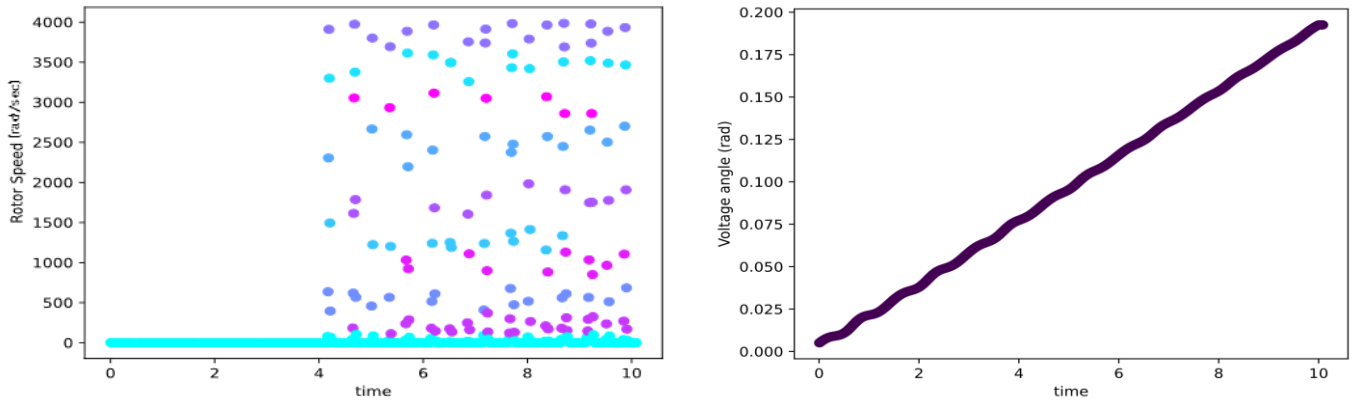


Figure 9. (**a**) Rotor angle and angular frequency of the first generator in IEEE 9-bus system under the DoS attack scenario 1; (**b**) rotor angle and angular frequency of the first generator in IEEE 9-bus system under the DoS attack scenario 2; (**c**) rotor angle and angular frequency of the first generator in IEEE 9-bus system under the DoS attack scenario 3; (**d**) rotor angle and angular frequency of the first generator in IEEE 9-bus system under the DoS attack scenario 4.

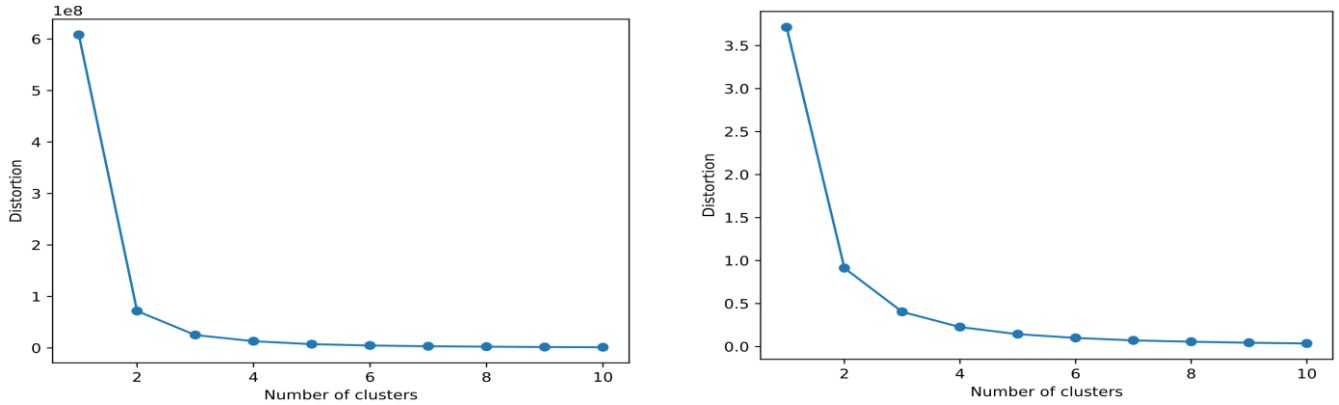
From Figure 8a–c, it is clear that the proposed method boosted the accuracy of the DSE, especially during the time of FDI cyber-attacks, a task in which both EKF and UKF performed poorly. It is worth noting that before the cyber-attack, all three methods accurately estimated the dynamic states of the network. After the cyber-attack was launched, however, Kalman filters failed to detect and eliminate the attacks. The situation deteriorates in the case of DoS attacks. From (a) to (d) subplots of Figure 9, it can be observed that the mentioned filters almost failed to eliminate the attacks, while the proposed DTR-based method properly detected and eliminated the attack vectors.

In Figure 10a, an example of an attacked dataset detected by the HC method is illustrated, while in Figure 10b, a feature is shown which is not attacked. Both of the mentioned figures are heatmaps plotted by scatter function in Python with "cmap" set to cool. The former is the rotor speed of the second generator, and the latter is the voltage angle of bus three. Figure 11a,b shows the clustering inertia of both mentioned features. The accuracy of the proposed method significantly depends on the accurate functioning of the clustering method, which diagnoses malfeatures.



(**a**) (**b**)

Figure 10. (**a**) Rotor speed of the second generator in IEEE 9-bus system under the FDI attack; (**b**) voltage angle of the third bus in IEEE 9-bus system.



(**a**) (**b**)

Figure 11. (**a**) Clustering inertia for the rotor speed of the second generator in IEEE 9-bus system under the FDI attack; (**b**) clustering inertia for the voltage angle of the third bus in IEEE 9-bus system under the FDI attack.

The proposed indices are calculated and compared to another related study in Tables 3 and 4 under different attack scenarios in the IEEE 3-machine 9-bus test system. It is worth noting that the method proposed in [12] is RCKF.

From Figure 11a,b, it is clear that as soon as the attacked measurement of rotor speed enters the HC, the distortion of only one cluster boosts rapidly, and the injected data is eliminated, while all of the voltage angle data are correct and the distortion for only one cluster is smaller than d. The second index has the same value for both rotor speed and angle, as it measures the detecting accuracy of HC and does not depend on any individual features. By taking the first index into account, the proposed method works slightly better than that of [12], which shows the higher accuracy of the proposed method.

From Tables 3 and 4, it can be seen that the HC-DTR-based dynamic state estimation outperformed the RCKF technique. The HC model managed to detect the attacked data better than the Kalman filter algorithm, and the DTR predicted the actual values more robustly than the method conducted in [12].

Figure 12 illustrates the generator's states in the IEEE 5-machine 14-bus under three different FDI attack scenarios, while Figure 13 shows the generator's states under DoS attack scenarios. In this test system, only UKF was employed as an alternative method due to the low accuracy of EKF.

Table 3. Indices calculated for the rotor angle of the first generator in IEEE 9-bus system.

Scenarios	Index	[12]	This Article
First FDI scenario	τ_1	6.0998×10^5	5.4721×10^5
	τ_2	×	0.9372
	τ_3	×	4.7548×10^6
Second FDI scenario	τ_1	6.4476×10^5	5.8539×10^5
	τ_2	×	0.9421
	τ_3	×	5.4152×10^6
Third FDI scenario	τ_1	6.8111×10^5	6.1836×10^5
	τ_2	×	0.9723
	τ_3	×	6.6205×10^6
First DoS scenario	τ_1	1.6683×10^4	1.3721×10^4
	τ_2	×	0.9936
	τ_3	×	1.0665×10^5
Second DoS scenario	τ_1	1.6640×10^4	1.4380×10^4
	τ_2	×	0.9632
	τ_3	×	2.4792×10^5
Third DoS scenario	τ_1	1.6549×10^4	1.5779×10^4
	τ_2	×	0.9248
	τ_3	×	3.6721×10^5
Fourth DoS scenario	τ_1	1.6378×10^4	1.6035×10^4
	τ_2	×	0.8931
	τ_3	×	4.9620×10^5

Table 4. Indices calculated for the rotor speed of the first generator in IEEE 9-bus system.

Scenarios	Index	[7]	This Article
First FDI scenario	τ_1	1.5821×10^5	1.2395×10^5
	τ_2	×	0.9372
	τ_3	×	2.1442×10^8
Second FDI scenario	τ_1	1.5841×10^5	1.3254×10^5
	τ_2	×	0.9421
	τ_3	×	6.5948×10^8
Third FDI scenario	τ_1	1.5969×10^5	1.4837×10^5
	τ_2	×	0.9723
	τ_3	×	9.9827×10^8
First DoS scenario	τ_1	1.5626×10^5	1.1147×10^5
	τ_2	×	0.9936
	τ_3	×	1.9546×10^7
Second DoS scenario	τ_1	1.5619×10^5	1.2759×10^5
	τ_2	×	0.9632
	τ_3	×	4.2756×10^7

Table 4. *Cont.*

Scenarios	Index	[7]	This Article
Third DoS scenario	τ_1	1.5612×10^5	1.4738×10^5
	τ_2	×	0.9248
	τ_3	×	6.9563×10^7
Fourth DoS scenario	τ_1	1.5604×10^5	1.5392×10^5
	τ_2	×	0.8931
	τ_3	×	1.6383×10^6

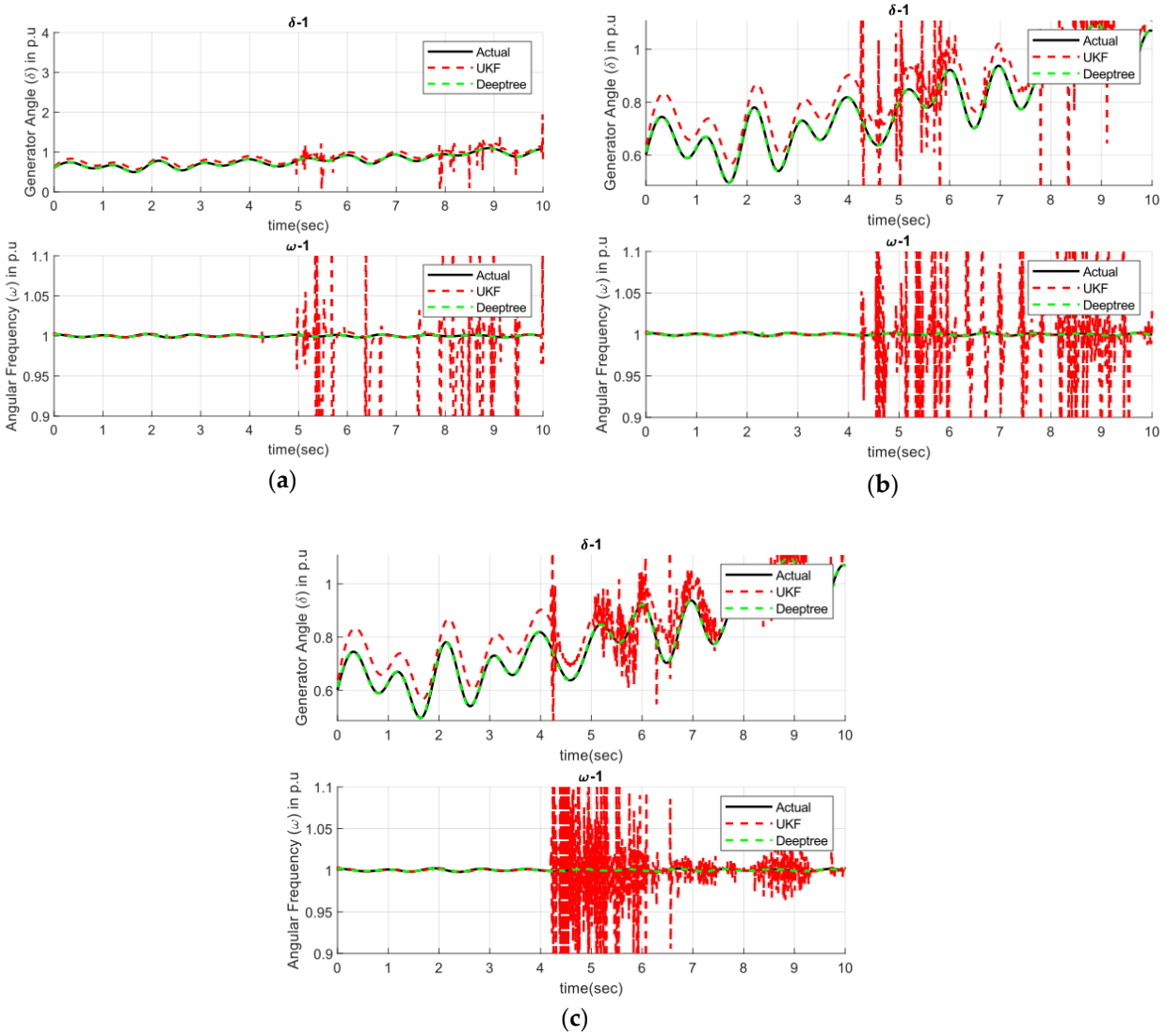


Figure 12. (**a**) Rotor angle and angular frequency of the first generator in IEEE 14-bus system under the FDI attack scenario 1; (**b**) rotor angle and angular frequency of the first generator in IEEE 14-bus system under the FDI attack scenario 2; (**c**) rotor angle and angular frequency of the first generator in IEEE 14-bus system under the FDI attack scenario 3.

As it is clear from Figure 12, the proposed machine learning-based method's accuracy is far better than the UKF's, even in more extensive scenarios under FDI attacks. Similar to the previous cyber-attack, it is clear from Figure 13 that the DoS attack is well detected and eliminated by the proposed method, a task in which the UKF has failed. The DTR method shows considerable potential in eliminating different cyber-attacks, as illustrated in the mentioned figures for both the IEEE 3-machine 9-bus test system and the IEEE 5-machine

14-bus test system. Figure 14 illustrates the rotor speed's data of the second generator and voltage angle's data of the third bus as attacked and the true features. Both mentioned figures are heatmaps plotted by scatter function in Python with "cmap" set to warm, while Figure 15 shows the cluster inertia of both features. It is worth noting that the HC method is clustering the data simultaneously, which is vitally essential for rapid response against cyber-attacks.

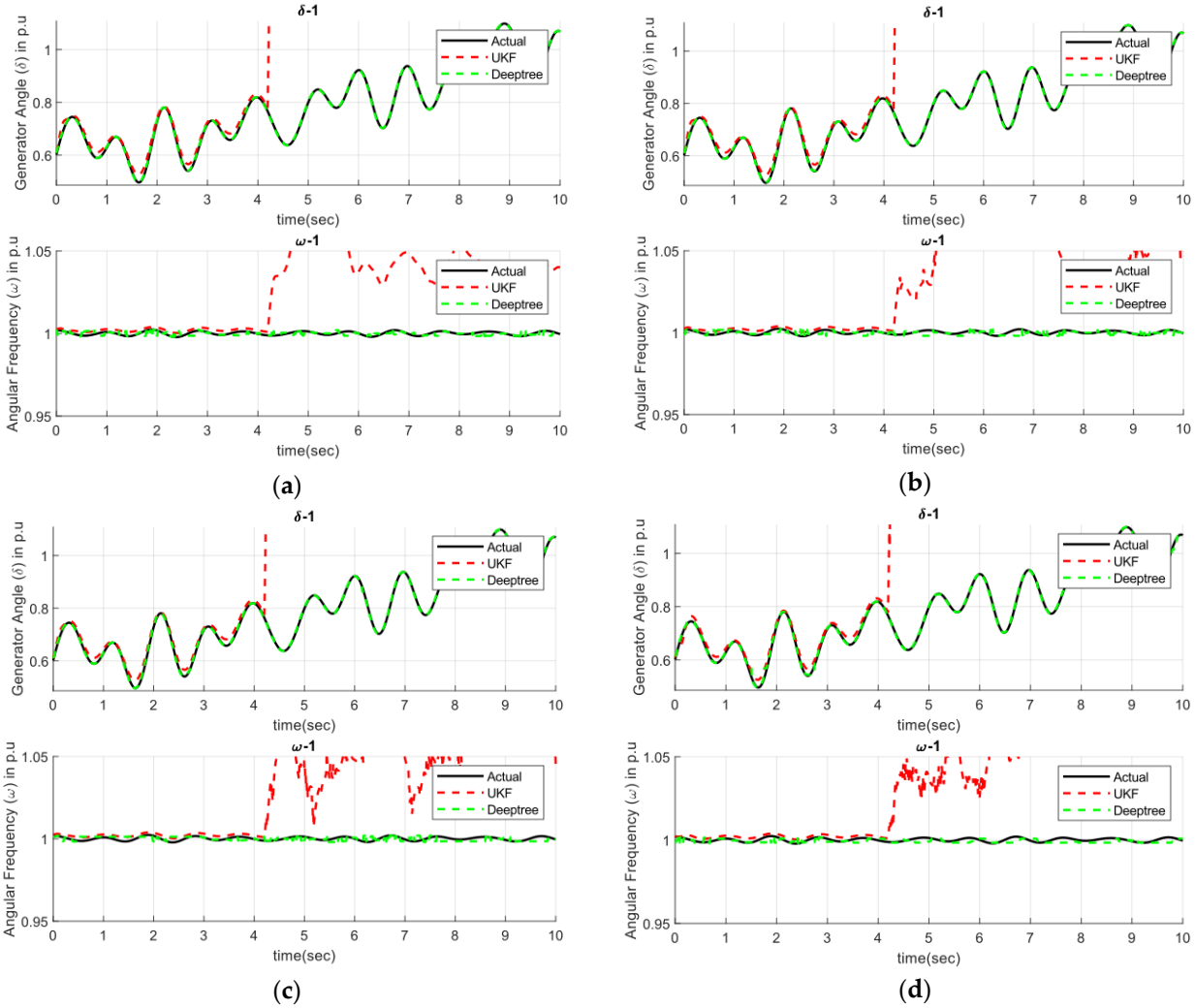
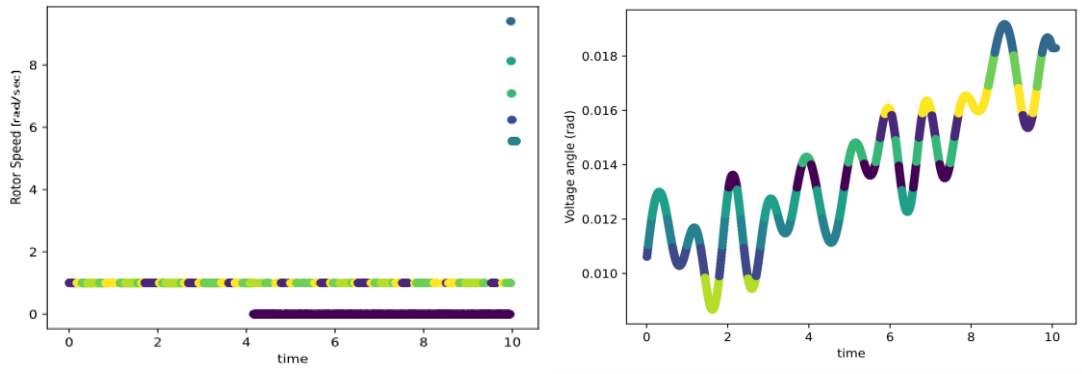


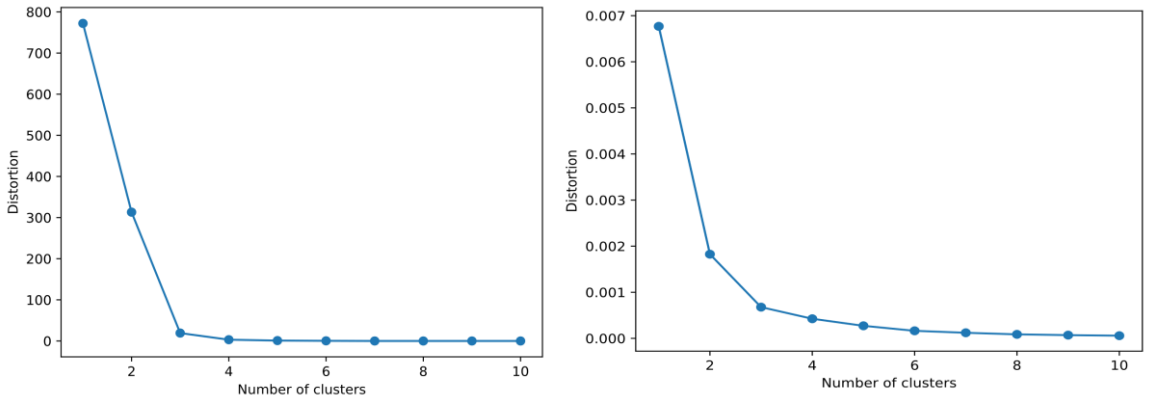
Figure 13. (**a**) Rotor angle and angular frequency of the first generator in IEEE 14-bus system under the DoS attack scenario 1; (**b**) rotor angle and angular frequency of the first generator in IEEE 14-bus system under the DoS attack scenario 2; (**c**) rotor angle and angular frequency of the first generator in IEEE 14-bus system under the DoS attack scenario 3; (**d**) rotor angle and angular frequency of the first generator in IEEE 14-bus system under the DoS attack scenario 4.

The proposed indices are illustrated in Tables 5 and 6 for rotor angle and rotor speed, respectively, and compared to results from two other related studies [36,37], for the IEEE 5-machine 14-bus test system. It is worth mentioning that [36] proposed a non-linear method based on a novel Kalman filter for detecting and eliminating the FDI attack, while [37] employed a support vector machine classification-based method for diagnosing the DoS attack.



(**a**) (**b**)

Figure 14. (**a**) Rotor speed of the second generator in IEEE 14-bus system under the DoS attack; (**b**) voltage angle of the third bus in IEEE 14-bus system.



(**a**) (**b**)

Figure 15. (**a**) Clustering inertia for the rotor speed of the second generator in IEEE 14-bus system under the DoS attack; (**b**) clustering inertia for the voltage angle of the third bus in IEEE 14-bus system.

Table 5. Indices calculated for the rotor angle of the first generator in IEEE 14-bus system.

Scenarios	Index	[36]	[37]	This Article
First FDI scenario	τ_1	×	×	6.2471×10^5
	τ_2	×	×	0.9163
	τ_3	×	×	1.5728×10^6
Second FDI scenario	τ_1	×	×	9.4638×10^5
	τ_2	×	×	0.9274
	τ_3	×	×	1.6371×10^6
Third FDI scenario	τ_1	×	×	1.2532×10^4
	τ_2	×	×	0.9355
	τ_3	2.4920×10^4	×	1.7814×10^6
First DoS scenario	τ_1	×	×	8.9060×10^5
	τ_2	×	×	0.9997
	τ_3	×	×	1.5406×10^6
Second DoS scenario	τ_1	×	×	9.7987×10^5
	τ_2	×	×	0.9723
	τ_3	×	×	1.6086×10^6

Table 5. *Cont.*

Scenarios	Index	[36]	[37]	This Article
Third DoS scenario	τ_1	×	×	1.0614×10^4
	τ_2	×	×	0.9491
	τ_3	×	×	1.6796×10^6
Fourth DoS scenario	τ_1	×	×	1.3000×10^4
	τ_2	×	0.9079	0.9186
	τ_3	×	×	2.2414×10^6

Table 6. Indices calculated for the rotor speed of the first generator in IEEE 14-bus system.

Scenarios	Index	[36]	[37]	This Article
First FDI scenario	τ_1	×	×	2.1461×10^5
	τ_2	×	×	0.9163
	τ_3	×	×	1.2362×10^7
Second FDI scenario	τ_1	×	×	3.6921×10^5
	τ_2	×	×	0.9274
	τ_3	×	×	1.5036×10^7
Third FDI scenario	τ_1	×	×	3.9251×10^5
	τ_2	×	×	0.9355
	τ_3	8×10^6	×	1.4270×10^7
First DoS scenario	τ_1	×	×	2.3250×10^5
	τ_2	×	×	0.9997
	τ_3	×	×	5.7519×10^7
Second DoS scenario	τ_1	×	×	3.7969×10^5
	τ_2	×	×	0.9723
	τ_3	×	×	6.5682×10^7
Third DoS scenario	τ_1	×	×	3.8801×10^5
	τ_2	×	×	0.9491
	τ_3	×	×	6.7121×10^7
Fourth DoS scenario	τ_1	×	×	4.0986×10^5
	τ_2	×	0.9079	0.9186
	τ_3	×	×	7.0902×10^7

It is clear from Tables 5 and 6 that the proposed method possesses better detection accuracy in the case of DoS attacks than that of [36] and more accuracy for estimating the dynamic states of the case study than that of [37]. Other indices illustrate that the proposed method is fully capable of eliminating DoS and FDI cyber-attacks and simply outperforms other mentioned techniques in [36,37].

6. Conclusions

A two-stage machine learning-based method was proposed in this paper to tackle the cyber-sabotage issue in the smart grid by clustering data using an HC method and regressing with DTR to eliminate the attack. This paper contributes to the area of DSE in power networks by using an unsupervised learning method for attack detection and an ensemble learning method for attack elimination. This novel technique was capable of detecting and eliminating cyber-attacks and tracking the dynamic states of the power

system, which can provide significant help to human operators to prevent them from making wrong decisions during the transient time in the power system operation. The proposed method carried out the given tasks better than previous methods based on the traditional Kalman filter and support vector machines. By correctly diagnosing the attack vectors, the proposed method provides the operators with accurate state estimations, decreasing the risk of blackouts or other disasters due to wrong commands. However, the full efficiency of the proposed method is yet to be tested in a large-scale power grid network, and the cost for this was not considered in the present study. Our future work will also focus on developing effective methods for distinguishing between faults, cyber-attacks, damaged PMUs, and measurement noise in power networks.

Author Contributions: Conceptualization, A.A., M.G. and A.A.G.; methodology, A.A. and M.G.; software, A.A.; validation, M.G., R.R.-F. and V.P.; formal analysis, M.G.; investigation, R.R.-F. and V.P.; resources, A.A.; data curation, A.A.; writing—original draft preparation, A.A.; writing—review and editing, R.R.-F. and V.P.; visualization, A.A.G.; supervision, M.G., R.R.-F. and V.P.; project administration, R.R.-F. and V.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

AI	Artificial Intelligence
CKF	Cubature Kalman Filter
DoS	Denial of Service
DSE	Dynamic State Estimation
DTR	Decision Tree Regressor
EKF	Extended Kalman Filter
FDI	False Data Injection
HC	Hierarchical Clustering
PMU	Phasor Measurement Unit
RCKF	Robust Cubature Kalman Filter
UKF	Unscented Kalman Filter

References

1. Thabet, A.; Boutayeb, M. On the Modeling and State Estimation for Dynamic Power System. *Int. J. Electron. Sci. Eng.* **2013**, *7*, 965–974.
2. Farajzadeh-Zanjani, M.; Hallaji, E.; Razavi-Far, R.; Saif, M. Generative adversarial dimensionality reduction for diagnosing faults and attacks in cyber-physical systems. *Neurocomputing* **2021**, *440*, 101–110. [CrossRef]
3. Farajzadeh-Zanjani, M.; Hallaji, R.E.; Razavi-Far, R.; Saif, M.; Parvania, M. Adversarial Semi-Supervised Learning for Diagnosing Faults and Attacks in Power Grids. *IEEE Trans. Smart Grid* **2021**, *12*, 3468–3478. [CrossRef]
4. Zhao, J.; Qi, J.; Huang, Z.; Meliopoulos, A.P.S.; Gomez-Exposito, A.; Netto, M.; Mili, L.; Abur, A.; Terzija, V.; Kamwa, I.; et al. Power System Dynamic State Estimation: Motivations, Definitions, Methodologies, and Future Work. *IEEE Trans. Power Syst.* **2019**, *34*, 3188–3198. [CrossRef]
5. Razavi-Far, R.; Farajzadeh-Zanjani, M.; Saif, M.; Chakrabarti, S. Correlation Clustering Imputation for Diagnosing Attacks and Faults With Missing Power Grid Data. *IEEE Trans. Smart Grid* **2019**, *11*, 1453–1464. [CrossRef]
6. Debs, A.S.; Larson, R.E. A Dynamic Estimator for Tracking the State of a Power System. *IEEE Trans. Power Appar. Syst.* **1970**, *PAS-89*, 1670–1678. [CrossRef]
7. Huang, Z.; Schneider, K.; Nieplocha, J. Feasibility studies of applying Kalman Filter techniques to power system dynamic state estimation. In Proceedings of the 2007 International Power Engineering Conference (IPEC 2007), Singapore, 3–6 December 2007; pp. 376–382.
8. Ghahremani, E.; Kamwa, I. Dynamic State Estimation in Power System by Applying the Extended Kalman Filter with Unknown Inputs to Phasor Measurements. *IEEE Trans. Power Syst.* **2011**, *26*, 2556–2566. [CrossRef]

9. Hassani, H.; Razavi-Far, R.; Saif, M.; Palade, V. Generative Adversarial Network-Based Scheme for Diagnosing Faults in Cyber-Physical Power Systems. *Sensors* **2021**, *21*, 5173. [CrossRef]
10. Hallaji, E.; Razavi-Far, R.; Saif, M. DLIN: Deep Ladder Imputation Network. *IEEE Trans. Cybern.* **2021**, 1–13. [CrossRef] [PubMed]
11. Hassani, H.; Hallaji, E.; Razavi-Far, R.; Saif, M. Unsupervised concrete feature selection based on mutual information for diagnosing faults and cyber-attacks in power systems. *Eng. Appl. Artif. Intell.* **2021**, *100*, 104150. [CrossRef]
12. Li, Y.; Li, Z.; Chen, L. Dynamic State Estimation of Generators under Cyber Attacks. *IEEE Access* **2019**, *7*, 125253–125267. [CrossRef]
13. An Unprecedented Cyberattack Hit the US Power Grid | WIRED. Available online: https://www.wired.com/story/power-grid-cyberattack-facebook-phone-numbers-security-news/ (accessed on 31 August 2021).
14. Liang, B.-M. A hierarchical clustering based global outlier detection method. In Proceedings of the 2010 IEEE Fifth International Conference on Bio-Inspired Computing: Theories and Applications (BIC-TA), Changsha, China, 23–26 September 2010; pp. 1213–1215. [CrossRef]
15. Qi, J.; Taha, A.F.; Wang, J. Comparing Kalman Filters and Observers for Power System Dynamic State Estimation With Model Uncertainty and Malicious Cyber Attacks. *IEEE Access* **2018**, *6*, 77155–77168. [CrossRef]
16. Wang, S.; Zhao, J.; Huang, Z.; Diao, R. Assessing Gaussian assumption of PMU measurement error using field data. *IEEE Trans. Power Del.* **2018**, *33*, 3233–3236. [CrossRef]
17. Li, Y.; Li, J.; Qi, J. Robust Cubature Kalman Filter for Dynamic State Estimation of Synchronous Machines under Unknown Measurement Noise Statistics. *IEEE Access* **2019**, *7*, 29139–29148. [CrossRef]
18. Taha, A.F.; Qi, J.; Wang, J.; Panchal, J.H. Risk Mitigation for Dynamic State Estimation Against Cyber Attacks and Unknown Inputs. *IEEE Trans. Smart Grid* **2016**, *9*, 886–899. [CrossRef]
19. Wang, X.; Luo, X.; Guan, X. Unknown cyber attack detection and isolation for power systems via Luenberger observer. In Proceedings of the 2017 4th International Conference on Information, Cybernetics and Computational Social Systems (ICCSS), Dalian, China, 24–26 July 2017; pp. 673–678. [CrossRef]
20. Lei, M.; Mohammadi, M. Hybrid machine learning based energy policy and management in the renewable-based microgrids considering hybrid electric vehicle charging demand. *Int. J. Electr. Power Energy Syst.* **2021**, *128*, 106702. [CrossRef]
21. Almasabi, S.; Bera, A.; Mitra, J. Dynamic State Estimation Aided By Machine Learning. In Proceedings of the 2019 IEEE Power & Energy Society General Meeting (PESGM), Atlanta, GA, USA, 4–8 August 2019; pp. 1–5. [CrossRef]
22. Ferrag, M.A.; Maglaras, L.; Moschoyiannis, S.; Janicke, H. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *J. Inf. Secur. Appl.* **2019**, *50*, 102419. [CrossRef]
23. Sun, K.; Hou, Y.; Sun, W.; Qi, J. *Power System Control Under Cascading Failures: Understanding, Mitigation, and System Restoration*; John Wiley & Sons: Hoboken, NJ, USA, 2018.
24. Befekadu, G.; Gupta, V.; Antsaklis, P.J. Risk-Sensitive Control Under Markov Modulated Denial-of-Service (DoS) Attack Strategies. *IEEE Trans. Autom. Control.* **2015**, *60*, 3299–3304. [CrossRef]
25. Lu, Z.; Yang, S.; Sun, Y. Application of extended fractional Kalman filter to power system dynamic state estimation. In Proceedings of the 2016 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), Xi'an, China, 25–28 October 2016; pp. 1923–1927. [CrossRef]
26. Gao, W.; Wang, S. On-line dynamic state estimation of power systems. In Proceedings of the North American Power Symposium 2010, Arlington, TX, USA, 26–28 September 2010; pp. 1–6. [CrossRef]
27. Tebianian, H.; Jeyasurya, B. Dynamic state estimation in power systems using Kalman filters. In Proceedings of the 2013 IEEE Electrical Power & Energy Conference, Halifax, NS, Canada, 21–23 August 2013; pp. 1–5. [CrossRef]
28. Nielsen, F. Chapter 8: Hierarchical Clustering. In *Introduction to HPC with MPI for Data Science*; Springer: Berlin/Heidelberg, Germany, 2016. [CrossRef]
29. Maree, R.; Geurts, P.; Piater, J.; Wehenkel, L. Random Subwindows for Robust Image Classification. In Proceedings of the 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05), San Diego, CA, USA, 20–25 June 2005; Volume 1, pp. 34–40. [CrossRef]
30. de Amorim, R.C.; Hennig, C. Recovering the number of clusters in data sets with noise features using feature rescaling factors. *Inf. Sci.* **2015**, *324*, 126–145. [CrossRef]
31. Classification and Regression Analysis with Decision Trees | by Lorraine Li | Towards Data Science. Available online: https://towardsdatascience.com/https-medium-com-lorrli-classification-and-regression-analysis-with-decision-trees-c43cdbc58054 (accessed on 31 August 2021).
32. Sauer, P.W.; Pai, M.A.; Chow, J.H. Power System Toolbox. In *Power System Dynamics and Stability: With Synchrophasor Measurement and Power System Toolbox 2e*; Sauer, P.W., Pai, M.A., Chow, J.H., Eds.; John Wiley & Sons: Hoboken, NJ, USA, 2017; pp. 305–325. [CrossRef]
33. Särkkä, S. *Bayesian Filtering and Smoothing*; Physical Books Available from Cambridge University Press and a Free Electronic Version Online; Cambridge University Press: Cambridge, UK, 2013.
34. Milano, F. An Open Source Power System Analysis Toolbox. *IEEE Trans. Power Syst.* **2005**, *20*, 1199–1206. [CrossRef]
35. Xue, D.; Jing, X.; Liu, H. Detection of False Data Injection Attacks in Smart Grid Utilizing ELM-Based OCON Framework. *IEEE Access* **2019**, *7*, 31762–31773. [CrossRef]

36. Chakhchoukh, Y.; Lei, H.; Johnson, B.K. Diagnosis of Outliers and Cyber Attacks in Dynamic PMU-Based Power State Estimation. *IEEE Trans. Power Syst.* **2019**, *35*, 1188–1197. [CrossRef]
37. Sakhnini, J.; Karimipour, H.; Dehghantanha, A. Smart Grid Cyber Attacks Detection Using Supervised Learning and Heuristic Feature Selection. In Proceedings of the 2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE), Oshawa, ON, Canada, 12–14 August 2019; pp. 108–112. [CrossRef]